ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ
INFORMATION TECHNOLOGY, COMPUTER SCIENCE AND MANAGEMENT



УДК 519.725+519.876.5 DOI 10.12737/10395

Корректирующая способность декодера мягких решений троичных кодов Рида - Маллера второго порядка при большом числе ошибок*

Н. С. Могилевская**
Донской государственный технический университет, г. Ростов-на-Дону, Российская Федерация

Correcting capacity of soft-decision decoder of ternary Reed – Muller second-order codes with a large number of errors ***

N. S. Mogilevskaya[1]**
[1]Don State Technical University, Rostov-on-Don, Russian Federation

Цель работы состоит в изучении корректирующей способности нового мягкого декодера кодов Рида — Маллера. Метод достижения цели заключается в экспериментальном исследовании декодера с использованием специально построенной имитационной модели помехоустойчивого канала передачи данных. Источник и приемник сообщений модели оперируют цифровыми данными, заданными полем F_3. Линия связи построенной модели в зависимости от настроек выдает цифровые или непрерывные сигналы. В случае непрерывных сигналов рассматриваются два варианта базовых искажений сигнала и их комбинации. Помехоустойчивость моделируемых каналов связи обеспечивается применением кодов Рида — Маллера второго порядка, заданных над полем F_3, и нового декодера мягких решений для этих кодов. Результаты проведенных имитационных экспериментов показали, что исследуемый декодер как в цифровых, так и в полунепрерывных каналах позволяет исправлять ошибок больше, чем гарантируется минимальным кодовым расстоянием. Наибольшую эффективность декодер показал при использовании его в полунепрерывных каналах связи. Корректирующая способность декодера значительно зависит от типа линии связи и вида искажений, поражающих сигналы, и не чувствительна к местоположению ошибок внутри кодового слова. Сделаны выводы о возможности использования нового декодера в каналах связи низкого качества для обеспечения помехоустойчивости, а также в ряде криптографических приложений.

Ключевые слова: троичный канал связи, троичные коды Рида — Маллера, декодер мягких решений, математическая модель канала связи, экспериментальное исследование корректирующей способности кода, исправление ошибок за границей половины минимального расстояния кода.

The research objective is to study the correcting capacity of a new soft decoder of Reed-Muller codes. The technique of achieving the goal is an experimental study of the decoder using a specially built simulation model of the antinoise data transfer channel. The model message source and receiver handle the numeric data identified in F_3 field. The communication line of the constructed model produces digital or continuous signals depending on the settings. In the case of continuous signals, two variants of the basic signal distortion and their combinations are considered. Noise immunity of the simulated communication link is provided by using Reed-Muller second-order codes identified over F_3 field, and the new soft-decision decoder for these codes. The results of the simulation experiments show that the decoder under study in both digital and semicontinuous channel allows correcting more errors than it is guaranteed by the minimum code distance. The decoder has proved the most effective in the semicontinuous communication channels. The decoder's correcting capacity depends heavily on the communication line type and on the signal distortion mode; it is not sensitive to the error location within the codeword. Conclusions are made on the use of the new decoder in the low-rated communication channels to provide noise immunity, and in a number of the cryptographic applications.

Keywords: ternary channel, ternary Reed-Muller codes, soft-decision decoder, mathematical model of communication channel, experimental research of the code correcting capability, error control out of the half minimum code distance.

Введение. В разнообразных системах передачи и хранения информации для ее защиты от искажений используются алгебраические помехоустойчивые коды [1–3]. Одной из актуальных задач в настоящее время является разработка для

---

* Работа выполнена в рамках инициативной НИР.
** e-mail: broshka@nm.ru
*** The research is done within the frame of the independent R&D.

известных кодов новых декодеров, которые обладают какими-либо преимуществами по сравнению с известными декодерами. К таким преимуществам может относиться, например, увеличение скорости работы декодера или повышение корректирующей способности кодека. Так, в последние годы для обеспечения помехоустойчивости актуально применение декодеров мягких решений (ДМР), особенность которых состоит в том, что принятые из канала данные вводятся в декодер, минуя демодулятор [1]. Обычно использование ДМР дает лучшие результаты по сравнению с декодированием жестких решений, когда на вход декодера поступают значения с выхода демодулятора, преобразующего данные из канала в слова над фиксированным конечным алфавитом. Эффективность ДМР основана на том, что в отсутствие демодулятора не накапливаются ошибки квантования, однако обычно декодеры с технологией ДМР обладают большей сложностью — например, [2].

В работе [4] построен мягкий декодер кодов Рида — Маллера второго порядка, заданных над полем Галуа F_3 (далее $RM_3(2, m)$, m — параметр кода). При этом за основу взят декодер двоичных кодов Рида — Маллера второго порядка В. М. Сидельникова и А. С. Першакова [5], обладающего значительной корректирующей способностью (он исследовался в работах [6–7]). Однако нет теоретической или экспериментальной оценки корректирующей способности нового алгоритма.

Цель данной работы состоит в экспериментальном исследовании корректирующей способности нового мягкого декодера [4] троичных кодов Рида — Маллера второго порядка при различных условиях его эксплуатации. Для достижения цели необходимо решить две задачи. Во-первых, построить модель канала с троичным входом. Источник и приемник сообщений данной модели оперируют цифровыми данными, заданными над полем F_3, а линия связи в зависимости от настроек выдает цифровые или непрерывные сигналы над полем комплексных чисел. Во-вторых, провести экспериментальное исследование корректирующей способности нового декодера при различных видах искажений кодовых слов. С этой целью используется программная реализация построенной модели троичного канала связи.

Модель троичного канала передачи данных с использованием канального ДМР-кода Рида — Маллера второго порядка. Рассмотрим элементы модели канала с троичным входом и схему прохождения данных по модели (рис. 1).

Источник сообщений выдает информационные векторы

$$\overline{m} = (m_1, m_2, ..., m_k) \in F_3^k ,$$

где F_3^k — линейное k-мерное пространство, заданное над полем Галуа F_3.

Затем в кодере канала эти векторы обрабатываются с использованием линейного блочного кода $RM_3(2, m)$ Рида — Маллера второго порядка длины n и размерности $k(<n)$, заданного над полем F_3.

Сформированные кодовые векторы $\overline{c} \in F_3^n$ поступают в передатчик, который служит интерфейсом к линии связи и преобразует векторы $\overline{c} \in F_3^n$ в

$$\overline{z} = (z_1, z_2, ..., z_n)(\in C_3^n) ,$$

где C — поле комплексных чисел, сигналы z_s, $s = 1,...,n$ принадлежат мультипликативной группе $C_3 = \left\{ e^{i\frac{2\pi}{3}q} \right\}_{q=0,1,2}$ корней третьей степени из единицы.

Преобразование аддитивной группы поля F_3 в мультипликативную группу C_3 происходит с помощью естественного изоморфизма $\phi : F_3 \to C_3$, который определяется по формуле

$\phi(j) = e^{i\frac{2\pi}{3}j}$, $j \in F_3$.

Сформированные векторы $\overline{z} = (z_1, z_2, ..., z_n)$ передатчик на физическом уровне отправляет в линию связи. Физический аналог сигнала z_j можно получить, например, с помощью модуляции с непрерывной фазой [2]. Диаграмма пространства таких сигналов иллюстрируется рис. 2.

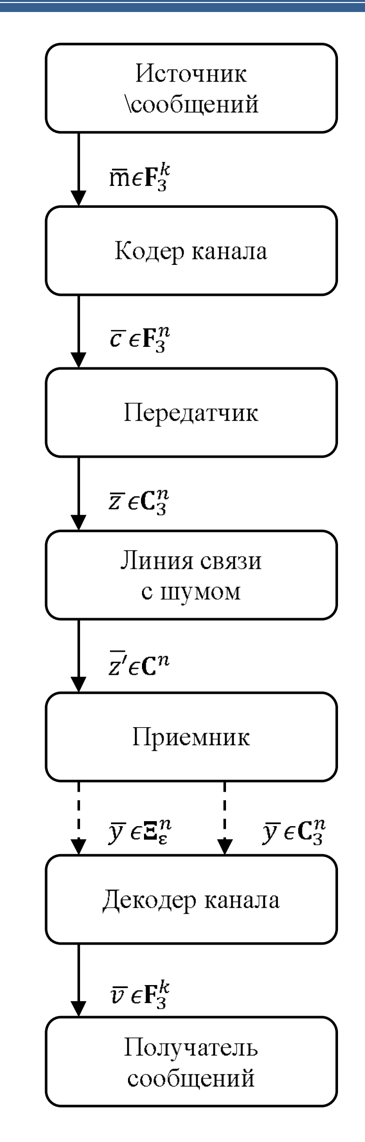


Рис. 1. Схема прохождения данных в моделируемом канале

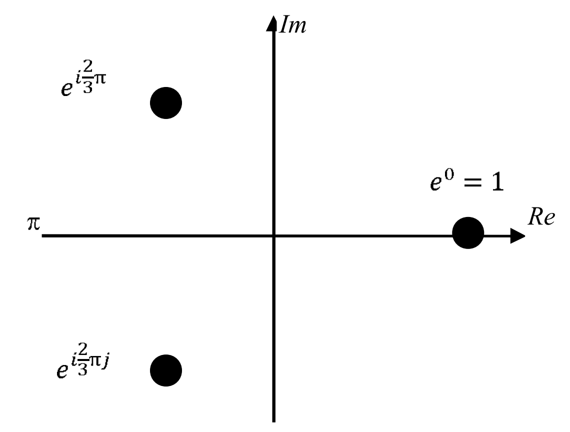


Рис 2. Диаграмма пространства сигналов

В силу искажений, действующих в линии связи, на выходе из нее формируются символы из поля *C*. Будем рассматривать два базовых вида искажений элементов вектора $\bar{z} \in C_3^n$ в линии связи — а именно, искажения по фазе и по амплитуде. Под искажением по фазе будем понимать фазовый сдвиг сигнала z_j по единичной окружности. Искажением по амплитуде будет смещение сигнала с единичной окружности по радиусу. Предположим, что под воздействием шума координаты вектора $\bar{z}$ подвергаются различным комбинациям базовых искажений и формируется вектор $\bar{z}' \in C^n$. Графическая иллюстрация искажений сигнала представлена в левой верхней четверти рис. 3. Так, сигнал $e^{i\frac{2\pi}{3}}$ показан черной точкой, голубая точка соответствует его искажению по амплитуде, зеленая — по фазе, а желтая — комбинации двух видов искажения.

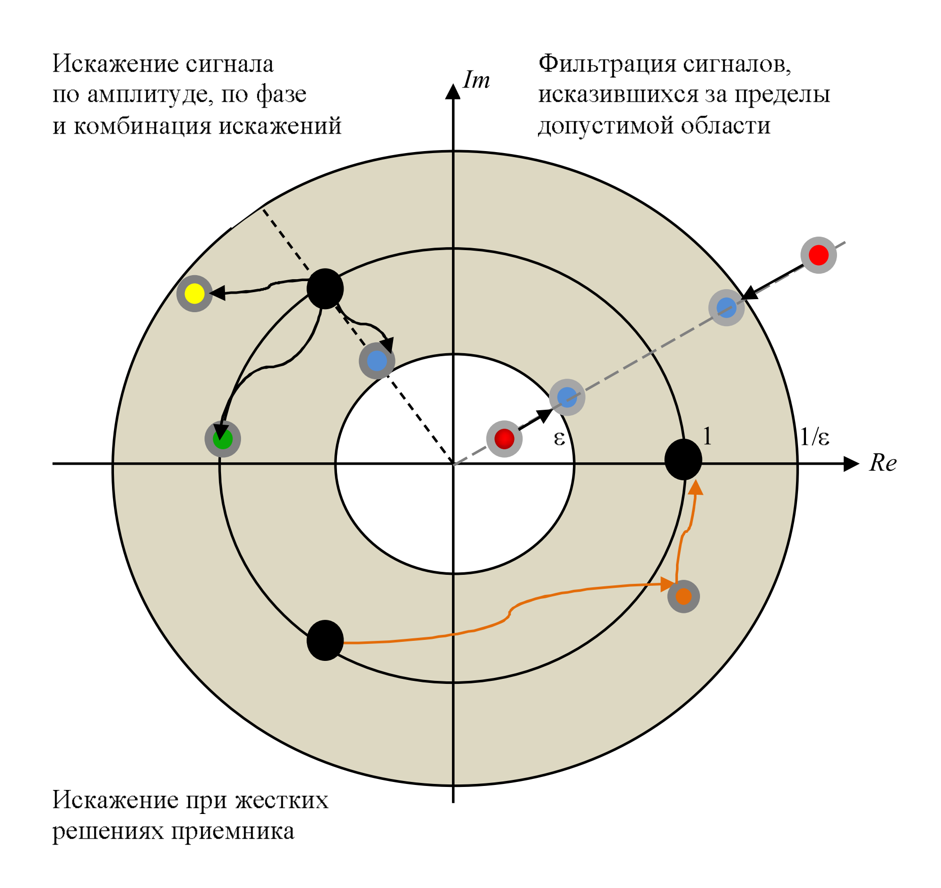


Рис. 3. Примеры искажения сигнала и его фильтрации

Вектор $\bar{z}' \in C^n$ поступает на вход приемника, который в зависимости от настроек может выдавать мягкие или жесткие решения о принятом сигнале. Так, в случае жестких решений приемник преобразует входной вектор $\bar{z}' \in C^n$ в вектор $\bar{y} = (y_1, ..., y_n) \in C_3^n$, независимо от типа искажений, поразивших вектор в линии связи. В этом случае может быть использован, например, принцип решающих областей. Таким образом, в результате воздействия ошибки символ $z_s = e^{i\frac{2\pi}{3}a} \in C_3$, $a \in F_3$ может перейти в один из двух других возможных символов: $y_s = e^{i\frac{2\pi}{3}b} \in C_3$, $b \in F_3$, $a \neq b$. В построенной реализации модели такой переход осуществляется равновероятно. На рис. 3 показано, что сигнал $e^{i\frac{4\pi}{3}}$, обозначенный черной точкой, в результате искажения перешел в сигнал, обозначенный коричневой точкой, а приемник с жесткими решениями преобразовал его в сигнал e^0.

В случае мягких решений приемник фильтрует амплитуду каждого сигнала z_s' таким образом, чтобы значения сигнала y_s на выходе приемника принадлежали допустимой области

$$\Xi_\varepsilon = \{\xi \in C \mid \varepsilon \leq |\xi| \leq 1/\varepsilon\},$$

где $\varepsilon (\in (0;1])$ — параметр приемника.

$\bar{y} = (y_1, ..., y_n) \in \Xi_\varepsilon^n$. Действие фильтра иллюстрируется на правой верхней четверти рис. 3: сигналы, обозначенные красными точками, попавшие в результате искажений в линии связи за пределы допустимой области, переводятся приемником в сигналы, лежащие в области допустимых значений, с помощью смещения их по радиусу к ближайшей точке на границе области Ξ_ε. Допустимая область выделена на рис. 3 серым цветом. Используя принятую в теории связи терминологию, можно говорить, что в случае работы приемника в режиме жестких решений реализуется цифровой канал, а в случае работы в режиме мягких решений — полунепрерывный канал.

Вектор $\bar{y}$ из пространства Ξ_ε^n или $C_3^n(\subset \Xi_\varepsilon^n)$ с выхода приемника (в зависимости от режима работы приемника) направляется в декодер мягких решений, цель которого — восстановить информационный вектор $\bar{m} \in F_3^k$, посланный ранее источником сообщений. Результат декодирования $\bar{v}(\in F_3^k)$ поступает получателю сообщения. В зависимости от уровня повреждения вектора $\bar{z}$ в канале связи результат декодирования может совпадать с исходным вектором или отличаться от него. Если $\bar{m} = \bar{v}$, то принято говорить о верном декодировании, иначе говорят об ошибке декодирования.

Определение кодов Рида — Маллера *RM*3(2,*m*). Используя [4], [8], определим троичный код Рида — Маллера *RM*3(2,*m*) второго порядка с параметром $m \geq 2$, следующим образом:

$$RM_3(r,m) = \{(f(\bar{\alpha}_1), ..., f(\bar{\alpha}_n)) \mid f \in F_3^{(2)}[x_1, ..., x_m]\} \in F_3^n,$$

где $n = 3^m$ — длина кода, множество

$$\{\bar{\alpha}_1, ..., \bar{\alpha}_n\} \left(\bar{\alpha}_j = (\alpha_{j_1}, ..., \alpha_{jm})\right) \quad (1)$$

представляет собой упорядочение всех точек векторного пространства F_3^m.

Далее в работе используем следующее упорядочение:

— по целочисленной сумме координат $\rho(\bar{\alpha})$ вектора $\bar{\alpha} \in F_3^m$ как натуральных чисел от меньшего к большему, а при одинаковых суммах — обычное лексикографическое упорядочение слева направо от большего к меньшему;

— $F_3^{(2)}[x_1, ..., x_m]$ — кольцо полиномов степени не выше 2 от *m* переменных над полем F_3.

Степень $\deg(f)$ полинома f определяется как максимальная степень составляющих его ненулевых мономов, а степень ненулевого монома $\phi = x_1^{\gamma_1} ... x_m^{\gamma_m} = a\bar{x}^{\bar{\gamma}}$ задается равенством $\deg(\phi) = \rho(\bar{\gamma})$.

Вектор $\bar{v} \in F_3^k$, где $k = 1 + m + C_{m+1}^2$, составленный из коэффициентов информационного полинома $v(\bar{x}) \in F_3^{(2)}[x_1, ..., x_m]$, называется информационным вектором. При этом предполагается, что для нумерации элементов информационного вектора, как и кодового, используется упорядочение (1). Кодирование информационного вектора осуществляется путем вычисления значений соответствующего информационного полинома в точках пространства F_3^m, упорядоченного в соответствии с (1). Способы нахождения числа гарантированно исправляемых ошибок в общем виде см. в [4], [8]. Далее в работе будем использовать уже вычисленные значения.

Конструкция ДМР для кодов *RM*3 (2,*m*). На вход алгоритма подаются параметр *m* кода *RM*3(2,*m*), связанные с *m* значения длины *n* и размерности k кода *RM*3 (2,*m*), а также полученный из канала зашумленный кодовый вектор $\bar{Y} = (Y_{\bar{\alpha}_1}, ..., Y_{\bar{\alpha}_n}) \in \Xi_\varepsilon^n(\subset C^n)$, элементы которого занумерованы в соответствии с (1). На выходе алгоритма формируется восстановленный информационный вектор $\bar{f}$.

Шаг 1. Построим набор векторов из $C^n : \{\nabla_{\bar{\gamma}}(\bar{Y}) = (Y_{\bar{\gamma}+\bar{\alpha}_1} Y_{\bar{\alpha}_1}^{-1}, ..., Y_{\bar{\gamma}+\bar{\alpha}_n} Y_{\bar{\alpha}_n}^{-1})\}_{\bar{\gamma} \in F_3^m, \bar{\gamma} \neq 0}$,

где $Y_{\bar{\alpha}_s}^{-1}$ — число, сопряженное $Y_{\bar{\alpha}_s}$, векторы $\bar{\gamma} \in F_3^m$ упорядочены по (1). Далее везде, где нумерация элементов векторов или наборов осуществляется векторными переменными из F_3^m, по умолчанию будем использовать упорядочение (1).

Шаг 2. Рассмотрим все значения $\bar{\gamma} \in F_3^m$, $\bar{\gamma} \neq \bar{0}$ и для фиксированного $\bar{\gamma}$ введем обозначение $\bar{P} = (P_{\bar{\alpha}_1}, ..., P_{\bar{\alpha}_n}) := \nabla_{\bar{\gamma}}(\bar{Y})$.

$B=(B_{\bar{\gamma}_1}=\bar{0},B_{\bar{\gamma}_2},...,B_{\bar{\gamma}_n})$ и $A=(A_{\bar{\gamma}_1}=\bar{0},A_{\bar{\gamma}_2},...,A_{\bar{\gamma}_n})$ B, где $B_{\bar{\gamma}}$ — вектор $\bar{\beta}=(\beta_1,...,\beta_m)\in F_3^m$, на котором достигается $A_{\bar{\gamma}}$ — минимальное значение функционала

$$A(\bar{P},\bar{\beta})=\sum_{s=1}^{n}\left|P_{\bar{\alpha}_s}-e^{i\frac{2}{3}\pi(\beta_0+\langle\bar{\beta},\bar{\alpha}_s\rangle)}\right|(\in R),$$

где $\langle\bar{\beta},\bar{\alpha}_s\rangle(\in F_3)$ — скалярное произведение, $\beta_0\in F_3$.

<u>Шаг 3.</u> Построим $(n\times m)$-массив Θ, строки которого инициализируем значениями из набора *B*: $\Theta(\bar{\alpha}_s)=B_{\bar{\alpha}_s}=(\theta_{1,\bar{\alpha}_s},...,\theta_{m,\bar{\alpha}_s})\in F_3^m$. Далее *j*-й столбец полученного массива будем обозначать Θ_j, $j=1,...,m$. Для каждого $\bar{\alpha}_s\in F_3^m$ и всех $\bar{\beta}_j\in F_3^m$ таких, что $\bar{\beta}_j\neq\bar{\alpha}_s$, вычислим

$$\Theta(\bar{\alpha}_s):=Maj(\Theta(\bar{\alpha}_s+\bar{\beta}_j)-\Theta(\bar{\beta}_j))_{\bar{\beta}_j\in F_3^m,\bar{\beta}_j\neq\bar{\alpha}_s},$$

где функция Maj возвращает элемент, встречающийся наибольшее число раз.

<u>Шаг 4</u>. Для каждого $j=1,...,m$ найдем d_j как минимум функционала

$$T_j(\phi)=\sum_{s=1}^{n}A_{\bar{\alpha}_s}\left|e^{i\frac{2}{3}\pi(2\phi(\bar{\alpha}_s)-\theta_{js})}-1\right|(\in R),$$

заданного на множестве всех линейных однородных полиномов вида $\phi(\bar{x})=\sum_{q=1}^{m}\phi_q x_q$, $\phi_q\in F_3$. Полином ϕ, на котором достигается минимум, обозначим $\omega^{(j)}(\bar{x})=\sum_{q=1}^{m}\omega_q^{(j)}x_q$.

Вычислим $\psi(\bar{x})=\sum_{q\le j}a_{qj}x_q x_j$, где $\bar{x}\in F_3^m$, $\grave{a}_{qj}\in F_3$, $q,j\in[1,...,m]$, $\grave{a}_{qj}=\grave{a}_{jq}$ и

$$a_{qj}=\begin{cases}\omega_j^{(q)}, если\ d_q<d_j\\ \omega_q^{(j)}, если\ d_q\ {}^3\ d_j\end{cases}.$$

<u>Шаг 5</u>. Среди множества векторов $\bar{\zeta}=(\zeta_1,...,\zeta_{ð})\in F_3^m$ и значений $\zeta_0\in F_3$ найдем те, которые минимизируют

$$\Phi(Y,\bar{\zeta})=\sum_{s=1}^{n}\left|Y_{\bar{\alpha}_s}-e^{i\frac{2}{3}\pi(\zeta_0+\langle\bar{\zeta},\bar{\alpha}_s\rangle+\psi(\bar{\alpha}_s))}\right|(\in R),$$

где $\langle\bar{\zeta},\bar{\alpha}_s\rangle(\in F_3)$ – скалярное произведение.

Из найденных значений составим полином $\varphi(\bar{x})=\sum_{j=1}^{m}c_j x_j+c_0$, где коэффициенты $c_k\in F_3$, $k=0,...,m$ соответствуют найденным значениям $\bar{\zeta}$ и ζ_0.

Результат декодирования строим в виде полинома: $f(\bar{x})=\psi(\bar{x})+\varphi(\bar{x})$, который определяет искомый информационный вектор $\bar{f}$.

Экспериментальное исследование. В работе проведено моделирование передачи закодированной информации по троичному каналу связи как с жесткими, так и с мягкими решениями приемника. Канал связи моделировался с использованием информационной системы «Канал» [9], для которой были созданы специальные библиотеки. При проведении экспериментов параметры модели задавались следующими входными данными:

— значение *m*, определяющее параметры помехоустойчивого кода $RM_3(2,m)$;

— число ошибок *t*, поражающих кодовое слово;

— тип приемника.

Если использовался приемник с мягкими решениями, то применялись дополнительные настройки, указывающие на вид используемых базовых искажений элементов кодовых слов, а также параметр приемника ε, задающий допустимую область значений Ξ_ε, при использовании искажений по амплитуде. Проведено 10^4 испытаний для каждого набора параметров модели.

Отметим, что при моделировании потоков ошибок часто используется понятие пораженных символов, т. е. попавших под воздействие искажений, но по случайности не изменивших своего значения [3], [10]. При проведении экспериментов такая ситуация намеренно не моделировалась, т. е. в результате наложения *t* ошибок на кодовое слово это слово отличалось от исходного ровно в *t* позициях.

В табл. 1 описаны основные параметры кодов $RM_3(2,m)$, результаты экспериментального исследования которых представлены ниже. В этой таблице использованы следующие обозначения: m — параметр кода $RM_3(2,m)$; n, k и t — длина, размерность кода и число гарантированно исправляемых ошибок (определяемое по минимальному расстоянию кода). Отношение t/n задает максимальное значение вероятности ошибки в канале связи, при котором код «гарантирует» выдачу верного результата. Отметим, что при ошибках, вероятность которых превышает t/n, классический детерминированный декодер всегда выдает ошибочные результаты. Параметр t/n показывает избыточность кода. При необходимости далее будем использовать традиционную краткую запись параметров кода в форме тройки $[n, k, d]$, где d — минимальное кодовое расстояние.

Таблица 1

Основные параметры кодов $RM_3(2,m)$, $m = 2, 3, 4, 5$

m	n	k	t	t/n	n/k
2	9	6	1	0,111	1,5
3	27	10	4	0,148	2,7
4	81	15	13	0,160	5,4
5	243	21	40	0,164	11,57
6	729	28	121	0,165	26,03

Проведенная серия экспериментов по определению корректирующей способности нового ДМР-кода $RM_3(2,m)$ в случае применения его в канале с жесткими решениями приемника показала значительное повышение числа исправляемых ошибок по сравнению с детерминированным декодером. Изменение значения максимальной вероятности исправляемых ошибок новым декодером по сравнению с детерминированным декодером представлено в табл. 2. В верхней строке таблицы указаны максимальные вероятности ошибок, исправление которых гарантируется кодом (параметр t/n, см. табл. 1). Вторая строка таблицы содержит максимальные вероятности ошибок, при которых новый мягкий декодер выдал верный результат во всех проведенных экспериментах (т. е. в 100 % случаев). Из приведенных результатов видно, что декодер значительно улучшил результат, гарантированный кодом, во всех случаях, кроме кода $RM_3(2,2)$. Так для $RM_3(2,3)$ корректирующая способность увеличилась на 34 %, для $RM_3(2,4)$ — на 54 %, а для $RM_3(2,5)$ — на 157 % (код гарантирует исправление 40 ошибок на кодовое слово, а декодер во всех проведенных экспериментах исправил все ошибки до 103 включительно на кодовое слово). Третья и четвертая строки таблицы отличаются от второй вероятностью выдачи декодером верного результата (третья строка — верный результат в 95 % случаев, четвертая — в 90 % случаев).

Таблица 2

Корректирующая способность нового декодера кода $RM_3(2, m)$
в случае применения его в канале с жесткими решениями приемника

Максимальное значение вероятности исправляемых ошибок, гарантируемое	Параметр кода $RM_3(2,m)$			
	$m = 2$	$m = 3$	$m = 4$	$m = 5$
кодом $RM_3(2,m)$	0,111	0,11	0,160	0,165
декодером с вероятностью 1	0,111	0,148	0,247	0,424
декодером с вероятностью 0,95	0,111	0,185	0,321	0,428
декодером с вероятностью 0,9	0,111	0,185	0,333	0,436

Для определения чувствительности нового ДМР-кода $RM_3(2,m)$ к различным базовым типам искажений и их комбинациям проведена серия экспериментов с различными настройками параметров модели канала связи. На рис. 4 представлен график зависимости вероятности верного декодирования от вероятности ошибки в канале связи для кода $RM_3(2,4)$.

Рассмотрим график подробнее. Кривая с подписью «Дискретные ошибки» отражает результаты экспериментов, проведенных в канале связи с жесткими решениями приемника. Напомним, что в этом случае ошибка переводит сигнал в один из двух других разрешенных сигналов из поля C_3. Кривая с подписью «Ошибки по фазе» отражает результаты экспериментов, проведенных в канале связи, где происходят только ошибки типа сдвига сигнала по фазе. Кривые с подписью «По фазе и амплитуде» отражают результаты экспериментов, проведенных в канале связи, где происходят различные комбинации ошибок по фазе и по амплитуде, в скобках указан параметр приемника ε, опреде-

ляющий ширину допустимой области Ξ_ε. Легко видеть, что чем меньше значение ε, тем область Ξ_ε больше. Эксперименты показали, что чем шире область допустимых значений (т. е. чем значения ε меньше), тем хуже корректирующая способность декодера. Однако для каждого кода находится такое значение ε, при увеличении которого значительного изменения корректирующей способности практически не происходит. Так для кода $RM_3(2,4)$ результаты экспериментов при значениях $\varepsilon \in [0.5, 1]$ практически неразличимы. На графике не представлена зависимость корректирующей способности декодера в случае, когда происходят только ошибки по амплитуде. Эксперименты показали, что декодер не чувствителен к таким ошибкам, если не происходит сдвига сигнала по фазе. Так, для числа ошибок типа по амплитуде от 1 до длины n кода декодер всегда выдает верный результат. Отметим, что взаимное положение кривых, представленных на графике, повторяется для различных кодов $RM_3(2,m)$, $m > 2$.

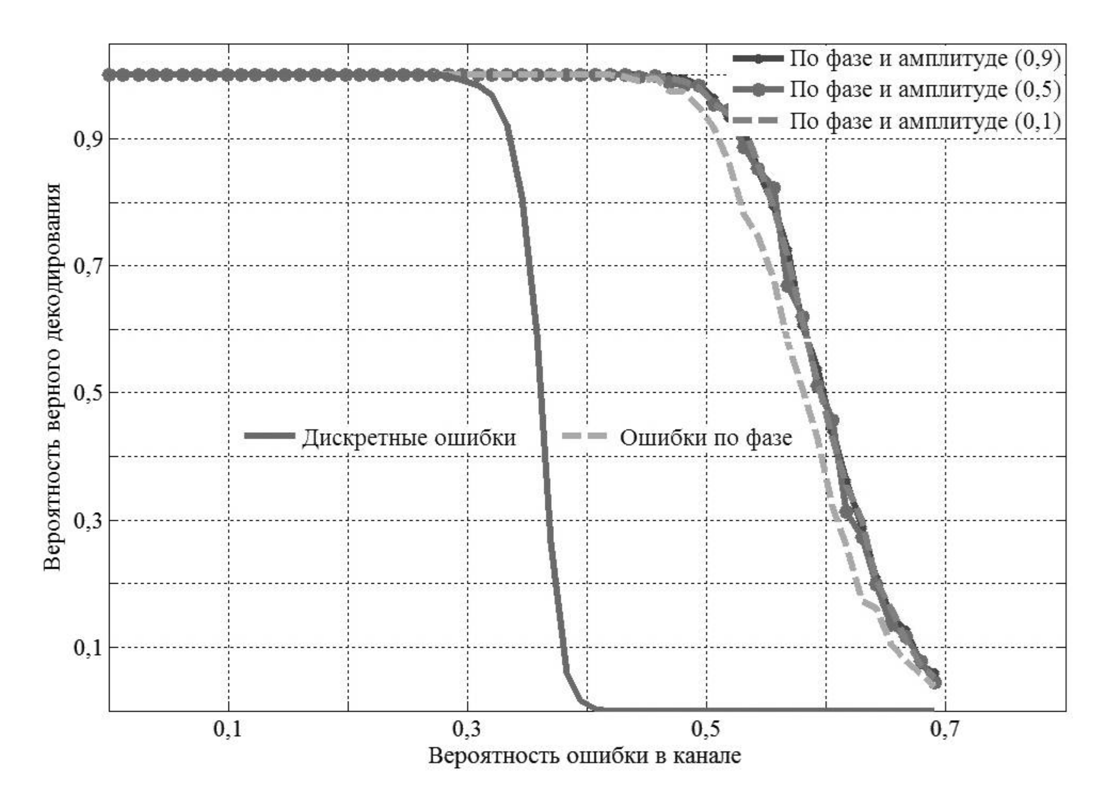


Рис. 4. Результаты исследования [81, 15, 27]-кода $RM_3(2,4)$

В работе проведена серия экспериментов по поиску зависимости корректирующей способности декодера от расположения ошибок внутри кодового слова. Результаты экспериментов показали, что декодер не чувствителен к местоположению ошибок.

Из табл. 1 видно, что [243, 21, 81]-код $RM_3(2,5)$ обладает достаточно высокой избыточностью $n/k = 11{,}6$. Возникает очевидный вопрос: целесообразно ли использовать этот код с его трудоемким алгоритмом декодирования или имеет смысл использовать коды с большой избыточностью и простыми декодерами? Рассмотрим в качестве кода, имеющего хорошую корректирующую способность и простой алгоритм мажоритарного декодирования, код повторения [1], [11] с близким значением избыточности и сравним корректирующие способности кода $RM_3(2,5)$ и [11,1,11]-кода многократного повторения над алфавитом F_3, который гарантированно исправляет 5 ошибок на 1 кодовое слово и обладает избыточностью, равной 11. Для того, чтобы сравнять длины кодовых слов обоих кодов, объединим 22 кодовых слова кода повторения — например, с помощью техники прямой суммы кодов [1], [11]. Таким образом, длина составного кодового слова — 242 символа, и код может гарантировано исправить 110 символов в этом составном слове, но только при жестком ограничении: ошибочные символы должны быть распределены внутри кодового слова равномерно (не более 5 ошибок на 11-символьный отрезок кодового слова). Код Рида — Маллера может гарантированно исправить только 40 ошибок внутри кодового слова длиной 234 символа, однако результат его работы не зависит от местоположения ошибок. Если использовать новый мягкий декодер кодов Рида — Маллера, то в рассматриваемом случае можно будет исправить 103 ошибки, также независимо от места их положения. Более того, если применять новый декодер в полунепрерывном канале связи, то декодер сможет исправить не менее 150 ошибок, вне зависимости от места их положения внутри кодового слова. Декодер кода многократного повторения не предназначен для исполь-

зования в полунепрерывном канале связи. Очевидно, что код многократного повторения, который обычно рассматривают как код, обладающий большой корректирующей способностью, уступает по этому параметру коду $RM_3(2,5)$, хотя, очевидно, выигрывает по скорости работы алгоритмов кодирования и декодирования. Для кодов $RM_3(2,m)$ с другими значениями параметра m аналогичные рассуждения также показывают выигрыш в корректирующей способности по сравнению с кодом многократного повторения. При этом с ростом m данный выигрыш растет, а с уменьшение значения m — падает.

Заключение. Результаты проведенных экспериментов показали, что исследуемый декодер троичного кода Рида — Маллера второго порядка обладает значительной корректирующей способностью по сравнению с классическими детерминированными декодерами — например, с декодированием по минимуму расстояния Хэмминга. Новый декодер мягких решений может быть применен для обеспечения помехоустойчивости в каналах связи низкого качества, используемых, однако, для передачи ценных сообщений. Так, на графике 4 видно, что даже при вероятности ошибки в канале связи, равной 0,5, т. е. значению, при котором говорят о разрыве линии связи, декодер выдает верные результаты с высокой достоверностью. Кроме традиционного применения декодера для обеспечения помехоустойчивости он может быть использован в таких практических приложениях, как восстановление информации, полученной по побочным (отводным) каналам связи [12], при построении криптосистем типа Мак-Элиса и Ниддерайтера [11].

Библиографический список

1. Морелос-Сарагоса, Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение / Р. Морелос-Сарагоса. — Москва : Техносфера, 2005. — 320 с.

2. Прокис, Дж. Цифровая связь / Дж. Прокис. — Москва : Радио и связь, 2000. — 800 с.

3. Деундяк, В. М. Имитационная модель цифрового канала передачи данных и алгебраические методы помехоустойчивого кодирования / В. М. Деундяк, Н. С. Могилевская // Вестник Дон. гос. техн. ун-та. — 2001. — Т. 1, № 1. — С. 98–104.

4. Деундяк, В. М. Модель троичного канала передачи данных с использованием декодера мягких решений кодов Рида — Маллера второго порядка / В. М. Деундяк, Н. С. Могилевская // Известия вузов. Северо-Кавказский регион. Технические науки. — 2015. — № 1. — С. 16–23.

5. Сидельников, В. М. Декодирование кодов Рида — Маллера при большом числе ошибок / В. М. Сидельников, А. С. Першаков // Проблемы передачи информации. — 1992. — Т. 28, № 3. — С. 80–94.

6. Loidreau, P. Modified version of Sidel'nikov-Pershakov decoding algorithm for binary second order Reed-Muller codes / P. Loidreau, B. Sakkour // Proc. Ninth International Workshop on Algebraic and Combinatorial Coding theory, ACCT-9. — Kranevo, 2004. — P. 266–271.

7. Могилевская, Н. С. Экспериментальное исследование декодеров кодов Рида — Маллера второго порядка / Н. С. Могилевская, В. Р. Скоробогат, В. С. Чудаков // Вестник Дон. гос. техн. ун-та. — 2008. — Т. 8, № 3. — С. 231–237.

8. Pellikaan, R. List decoding of q-ary Reed-Muller Codes / R. Pellikaan, X.-W. Wu // IEEE Transactions on Information Theory. — 2004. — Vol. 50 (1). — P. 679–682.

9. Информационная система «Канал» : св-во о гос. регистрации программ для ЭВМ № 2008614602 / Н. С. Могилевская, К. А. Чугунный ; заявл. 31.07.08 ; зарегистрир. 24.09.08. — 17 с.

10. Деундяк, В. М. Математическое моделирование источников ошибок цифровых каналов передачи данных: учеб. пособие / В. М. Деундяк, Н. С. Могилевская. — Ростов-на-Дону : Издательский центр ДГТУ, 2006. — 70 с.

11. Могилевская, Н. С. Введение в теорию информации: учеб. пособие / Н. С. Могилевская. — Ростов-на-Дону : Издательский центр ДГТУ, 2013. — 125 с.

12. Деундяк, В. М. О стойкости кодового зашумления к статистическому анализу наблюдаемых данных многократного повторения / В. М. Деундяк, Ю. В. Косолапов // Моделирование и анализ информационных систем. — 2012. — Т. 19, № 4. — С. 110–127.

References

1. Morelos-Zaragoza, R. Iskusstvo pomekhoustoychivogo kodirovaniya. Metody, algoritmy, primenenie. [The Art of Error Correcting Coding. Methods, algorithms, application.] Moscow: Tekhnosfera, 2005, 320 p. (in Russian).

2. Proakis, J. Tsifrovaya svyaz'. [Digital Communications.] Moscow: Radio i svyaz', 2000, 800 p. (in Russian).

3. Deundyak, V.M., Mogilevskaya, N.S. Imitatsionnaya model' tsifrovogo kanala peredachi dannykh i algebraicheskie metody pomekhoustoychivogo kodirovaniya. [Simulation model of digital data transmission channel and algebraic methods for error-correcting coding.] Vestnik of DSTU, 2001, vol. 1, no. 1, pp. 98–104 (in Russian).

4. Deundyak, V.M., Mogilevskaya, N.S. Model' troichnogo kanala peredachi dannykh s ispol'zovaniem dekodera my-

agkikh resheniy kodov Rida — Mallera vtorogo poryadka. [Ternary data channel model using the soft-decision decoder of Reed - Muller second-order codes.] Izvestiya vuzov. Severo-Kavkazskiy region. Technical Sciences. 2015, no. 1, pp. 16–23 (in Russian).

5. Sidelnikov, V.M., Pershakov, A.S. Dekodirovanie kodov Rida — Mallera pri bol'shom chisle oshibok. [Decoding of Reed - Muller Codes with a Large Number of Errors.] Problems of Information Transmission, 1992, vol. 28, no. 3, pp. 80–94 (in Russian).

6. Loidreau, P., Sakkour, B. Modified version of Sidel'nikov-Pershakov decoding algorithm for binary second order Reed-Muller codes. Proc. Ninth International Workshop on Algebraic and Combinatorial Coding theory, ACCT-9. Kranevo, 2004, pp. 266–271.

7. Mogilevskaya, N.S., Skorobogat, V.R., Chudakov, V.S. Eksperimental'noe issledovanie dekoderov kodov Rida — Mallera vtorogo poryadka. [Experimental study of second-order Reed-Muller codes.] Vestnik of DSTU, 2008, vol. 8, no. 3, pp. 231–237 (in Russian).

8. Pellikaan, R., Wu, X.-W. List decoding of q-ary Reed-Muller Codes. IEEE Transactions on Information Theory, 2004, vol. 50 (1), pp. 679–682.

9. Mogilevskaya, N.S., Chugunny, K.A. Informatsionnaya sistema «Kanal» : sv-vo o gos. registratsii programm dlya EVM № 2008614602. [Information system Channel: Certificate of Software State Registration no. 2008614602, 2008.] (in Russian).

10. Deundyak, V.M., Mogilevskaya, N.S. Matematicheskoe modelirovanie istochnikov oshibok tsifrovykh kanalov peredachi dannykh: ucheb. posobie. [Mathematical modeling of error sources of digital data channels: study guide.] Rostov-on-Don: DSTU Publ. Centre, 2006, 70 p. (in Russian).

11. Mogilevskaya, N.S. Vvedenie v teoriyu informatsii: ucheb. posobie. [Introduction to the theory of information: study guide.] Rostov-on-Don: DSTU Publ. Centre, 2013, 125 p. (in Russian).

12. Deundyak, V.M., Kosolapov, Y.V. O stoykosti kodovogo zashumleniya k statisticheskomu analizu nablyudaemykh dannykh mnogokratnogo povtoreniya. [On the Firmness Code Noising to the Statistical Analysis of the Observable Data of Repeated Repetition.] Modelirovanie i analiz informatsionnykh system, 2012, vol. 19, no. 4, pp. 110–127 (in Russian).

Поступила в редакцию 29.10.2014
Сдана в редакцию 06.11.2014
Запланирована в номер 28.01.2015